UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/069,714	04/26/2002	Michael John Hill	16673-7	4005

7590 12/08/2005

Clifford W Browning
Woodard Emhardt Naughton Moriarty & McNett
Bank One Center Tower
111 Monument Circle Suite 3700
Indianapolis, IN 46204-5137

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/069,714	HILL ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 are canceled.

Claims 11-20 are newly added and are examined.

Response to Amendment

2. Applicant's arguments filed 9/9/2005 regarding the rejection of the claims 1-10 under 35 U.S.C. 102() and 103 () have been fully considered but they are not persuasive.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Applicant mainly argues that that the Coppersmith et al. operations are performed sequentially, and each module operates with the complete result of the preceding module and that a module from the Coppersmith et al. chain does not start operating before the preceding one has terminated.

The examiner responds that the pending claims do not require starting operation of encryption/decryption module before the preceding one has terminated.

Claim 11 recites " a encryption/decryption module, different from the first module, starts encryption/ decryption operations as soon as said module receives a part of the results of encryption/decryption operations from the immediately preceding encryption/decryption module". The Examiner does not read this limitation to mean "starts of operation before the preceding one has just terminated". Furthermore a complete block encryption/decryption by each module constitutes claimed " partial

results " because a block encryption/decryption is considered partial results of sequence of input blocks of plaintext or ciphertext disclosed by Coppersmith.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 11-14 are rejected under 35 U.S.C. 102(b) as being unpatentable by prior art of record US Patent 5, 768,390 to Coppersmith et al. (hereinafter "Coppersmith")

As per claim 11, Coppersmith discloses method of encryption and decryption (Abstract) carried out by a plurality of encryption/decryption modules arranged in series (col. 3, lines 29-33 and Fig. 1 and 2), wherein a encryption/decryption module, different from the first module, starts encryption/decryption operations as soon as said module receives a part of the results of encryption/decryption operations from the immediately preceding encryption/decryption module (col. 5, lines 34-49, and col. 1, lines 41-46).

As per claim 12, Coppersmith discloses method according to Claim 11, wherein a decryption module, different from the first module, starts decryption operations as soon as said module receives a part of the results of decryption operations from the immediately preceding decryption module (col. 4, line 60 through col. 5, line 8).

As per claim 13, Coppersmith discloses method according to Claim 11, wherein an encryption module, different from the first module, starts encryption operations as soon as said module receives a part of the results of encryption operations from the immediately preceding encryption module (col. 5, lines 34-52 and Fig. 4).

As per claim 14, Coppersmith discloses method according to Claim 11, carried out by three modules wherein the central module operates with a secret symmetric key (A1, S, A2), (col. 6, lines 59-64 and item 710 of Fig. 7/ three decipherment steps using K1-k3) the central module (S) being of the type with secret symmetric key (k). (col. 6, lines 64-67/DES is a symmetric key encryption which uses the same keys for encryption/decryption).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 15-19 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Coppersmith et al in view of Menezes; Van Orschot, Vanstone. Hand Book of Applied Cryptography, 1967, CRC Press, 5th Edition 283-291(hereinafter "Menezes").

AS per claim 15, Coppersmith does not discloses but Menezes discloses method according to claim 14, wherein the first module and the last module in respect of encryption and in reversed order the last module and the first module in respect of decryption operate with an algorithm using asymmetric keys including a private key and a public key (Menezes page 286,8.4, where Menezes discloses using RSA for protecting messages sent over insecure channel using public key to encrypt the message and private key to decrypt the message).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Coppersmith system with the teaching of Menezes to

use RSA algorithm in the encryption modules of Coppersmith to substitute for symmetric encryption modules to overcome the problem of exchanging the decryption keys securely while maintaining the same level of data confidentiality. Furthermore, using symmetric and asymmetric encryption on the same cipher makes it harder for attackers to obtain the private key.

As per claims16 and 19, Menezes teaches using RSA as described in claim 15 where the private key is used for encryption and the public key is used for decryption (page 286, 8.1 and 8.3).

As per claim 17, Coppersmith as modified discloses method according to claim 16, wherein the first module and the last module use the same set of private and public keys (col. 4, lines 60 through col. 5, line 7/first encryption is preformed using K1 and the last encryption is performed using the same K1 as well).

As per claim 18, Coppersmith as modified discloses method according to Claim 16, wherein the first module and the last module use a different set of private and public keys (col. 6, line 59 through col. 7, line 7/the first module uses K1 and the last module uses K3 rather than K1).

5. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith as applied to claim 11 above, and further in view of Golstein et al. US Patent 6,128,735 (prior art of record).

As per claim 20, Coppersmith doe not disclose but Goldstein discloses method according to Claim 11, carried out by three encryption/decryption modules, wherein all three modules operate with asymmetric keys (Golstein discloses a method for transferring

data having different sensitivity level (see abstract) where he teaches the using of encryption using RSA (col. 3, lines 53-66)).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify coppersmith method with the teaching of Goldstein to implement all the modules in the system to support asymmetric key encryption because using asymmetric key would eliminate the risk of the shared key being compromised during exchange by enabling the system to communicate securely with other systems by using their public keys. Additionally using asymmetric and symmetric keys in the system enables the system to provide backward capability with system that just provide one method for encryption decryption.

Action is Final

6. **THIS ACTION IS FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131
12/4/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100